UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/609,019	06/30/2000	Yacov Yacobi	MS-65/1(116619.2)	2129

22801 7590 10/27/2003

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	**PAPER NUMBER**
2171	

DATE MAILED: 10/27/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/609,019	YACOBI ET AL.	
	Examiner	Art Unit	
	Brandon Hoffman	2171	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-55* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *41-52* is/are allowed.

6)☒ Claim(s) *1-19,21-29,31-40,53 and 54* is/are rejected.

7)☒ Claim(s) *14,20,26,27,30,51 and 55* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 June 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *2* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Drawings

1. The drawings are objected to under 37 CFR 1.83(a) because they fail to show the details of figures 8-17 as described in the specification. There is only mention to figures 1-15 in the specification. Also, from figure 8-15, in the specification, the figure is not representative of what is being depicted. Any structural detail that is essential for a proper understanding of the disclosed invention should be shown in the drawing. MPEP § 608.02(d).

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: Memory Storage Device 250 from page 20 and Digital Matrix Multiplier 406 from page 25.

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: Figure 2, reference number 261 (sound card) and 262 (speakers). A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in the description, are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

2. The disclosure is objected to because of the following informalities:

- On page 4, line 23, "White Paper" is written twice. Please remove one of these occurrences.
- On page 6 –
    - Line 9, the Authentication and Key Exchange Subsystem is missing its reference number. Please add reference number 116.
    - Lines 11, 15, and 23, Content Cipher Subsystem is missing its reference number. Please add reference number 120.
- On page 15, the reference to figures 10-15 is not correct. There are 17 figures and reference is made to only 15 of them. Also, the reference to figures 10-15 is not the same as what is depicted in the figures.
- On page 17, lines 14 and 26, and page 26, lines 9 and 13, the reference to PC 200 should be PC 220.
- On page 18, line 31, the System Bus is missing its reference number. Please add reference number 223.
- On page 19, line 13, System Bus 248 should be System Bus 223.
- On page 29 –
    - Line 6, and page 33, line 26, the Video Signal Encryption Circuit is missing its reference number. Please add reference number 406.
    - Line 7, the Pseudo-Random Number Generator is missing its reference number. Please add reference number 410.

- On page 34, there are multiple instances where Display Adapter and Display Device are missing their reference numbers. They should be 248 and 247, respectively. Please fix all these occurrences.
- On page 36 –
    - Line 21, the Authentication and Key Exchange System is missing its reference number. Please add reference number 516.
    - Lines 23 and 25, and page 37, line 2, the Pseudo-Random Number Generator is missing its reference number. Please add reference number 510.

Appropriate correction is required.

The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Claim Objections

3. Claims 14, 26, 27, and 51 are objected to because of the following informalities:

Regarding claim 14, "though" should be – through –.

Regarding claim 26, this dependent claim makes reference to claim 19. The correct dependency should be to claim 25.

Regarding claim 27, this claim is dependent upon claim 26, and therefore inherits its deficiencies.

Regarding claim 51, on line 8, there is a period (.) before the word "wherein". Please remove the period from this claim.

Appropriate correction is required.

The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not). Misnumbered claim 38 has been renumbered to 39.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 39 and 40 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 39 recites the limitation "the IEEE 1394 bus" on page 69, first line. There is insufficient antecedent basis for this limitation in the claim.

Claim 40 is dependent upon claim 39 and therefore inherits its deficiencies.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent, or
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1 and 2 are rejected under 35 U.S.C. 102(a/e) as being anticipated by Thue (U.S. Patent No. 6,002,707).

Regarding claim 1, Thue teaches a method of processing first, second and third signals for use in a system having first, second, and third signal lines (figure 1), comprising:

- Generating, using a pseudo-random number generator, pseudo-random output values (figure 1, reference number 130)
- Changing, as a function of at least one of said pseudo-random output values, which ones of the first, second, and third signal lines are used to transmit the first, second and third signals (figure 1, reference number 130 and column 2, lines 6-24).

Regarding claim 2, Thue teaches modifying at least one of the first, second or third signals, as a function of said one pseudo-random output value, prior to transmission of said one signal over one of said first, second, and third signal lines (figure 1, reference number 130).

Claims 36 and 37 are rejected under 35 U.S.C. 102(a/e) as being anticipated by Kohn et al. (U.S. Patent No. 6,570,990).

Regarding claim 36, Kohn et al. teaches a device (figure 9), comprising:

- A video signal encryption circuit for encrypting (figure 9, reference number 121), in response to a pseudo-random number, red, green and blue video signals and for producing first, second and third analog encrypted video signals;
- A pseudo-random number generator circuit (figure 9, reference number 200), coupled to the video signal encryption circuit, for producing the pseudo-random number value; and
- An input/output interface (figure 9, reference number 133) for outputting the first, second and third encrypted analog video signals.

Regarding claim 37, Kohn et al. teaches the device of claim 36, further comprising:

- Means for communicating with a destination device for establishing a session key to be used for encrypting and decrypting the red, green and blue analog encrypted video signals (figure 8, reference number 130 or 135).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Thue in view of Maeshima et al. (U.S. Patent No. 6,486,923).

Regarding claim 3, Thue teaches all of the subject matter of claims 1 and 2, as discussed above. However, Thue does not disclose the changing and modifying steps being performed by a matrix multiplication operation on the first, second, and third signals.

Maeshima et al. teaches the changing and modifying steps are performed by a matrix multiplication operation performed on the first, second, and third signals, the matrix multiplication operation utilizing matrix coefficients generated from a plurality of the pseudo-random output values (figure 1, reference number 50).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the pseudo-randomly generated matrix coefficients and the matrix multiplication operation using the coefficients, as taught by Maeshima et al. to the method of Thue. It would have been obvious to combine the pseudo-randomly generated matrix coefficients and the matrix multiplication operation using the

coefficients as taught by Maeshima et al. to the method of Thue because the pseudo-randomly generated matrix coefficients give a randomness to the encryption and the matrix multiplication operation using the coefficients allows a way to modify the red, green, and blue signals in order to encrypt the video signals (see column 3, lines 21-23 of Maeshima et al.).

Claims 4, 5, 7-12 are rejected under Thue as modified by Maeshima et al. in view of Kohn et al.

Regarding claims 4 and 9, Thue as modified by Maeshima et al teaches the limitations of claim 3, as noted above. However, Thue/Maeshima et al. do not disclose the provisions of the first, second, and third signal lines coupling a source device to a destination device, the pseudo-random number generator contained within the source device, and the device operating the source to communicate with the destination device to establish a key, and operating the pseudo-random number generator to generate pseudo-random output values.

Kohn et al., on the other hand, teaches such provisions:

- The first, second, and third signal lines couple a source device to a destination device, said pseudo-random number generator contained within the source device (figure 1, reference number 120 and figure 2, reference number 200), the method further comprising:
    - Operating the source device to communicate with the destination device so as to establish a session key (figure 6, reference number 529); and

- Operating the pseudo-random number generator to generate said pseudo-random output values as a function of the established session key (figure 6, reference number 530).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the provisions of Kohn et al. to the method of Thue as modified by Maeshima et al. It would have been obvious to combine the provisions as taught by Kohn et al. to the method of Thue as modified by Maeshima et al. because coupling signal lines from source device to destination device while having the pseudo-random number generator in the source device provides a means to encrypt data in the source device before transmission to the destination device. Operating the source device to communicate with the destination device to establish a session key is needed in encryption/decryption devices in order for proper decryption to take place. Generating pseudo-random output values as a function of the session key goes hand in hand with why the session key is determined between source and destination device. Once the session key is agreed upon, in encryption/decryption devices, that key is used as a seed for a pseudo-random number generator to provide random data that is a direct result of the session key.

Regarding claim 5, Thue as modified by Maeshima et al. in view of Kohn et al. teaches:

- The first, second, and third signals correspond to color signals representing an image (see figure 9 of Kohn et al.), the method further comprising:
    - Utilizing a different session key for each line of an image that is transmitted (see figure 6, reference numbers 555 and 560 of Kohn et al.).

Regarding claim 7, Thue as modified by Maeshima et al. in view of Kohn et al. teaches:

- The destination device includes an additional pseudo-random number generator (see figure 10, reference number 300 of Kohn et al.), the method further comprising:
    - Operating the destination device to perform, as a function of an output of the additional pseudo-random number generator, the inverse of the changing and modifying steps performed by the source device to restore the first, second and third signals to their original condition so as to yield restored first, second and third signals (see figure 10 of Kohn et al.).

Regarding claim 8, Thue as modified by Maeshima et al. and Kohn et al. teaches:

- The first, second and third signals are analog red, green and blue color video signals, respectively (see figure 9 of Kohn et al.), and the destination device is a computer monitor (see figure 8, reference number 160 of Kohn et al.);

- The method further comprising: displaying, on a display screen included in the destination device, an image represented by restored first, second and third color video signals (see figure 8, reference number 160); and
- The source device is a display adapter (see figure 8, reference number 152 of Kohn et al.).

Regarding claim 10, Thue as modified by Maeshima et al. in view of Kohn et al. teaches:

- Operating the source device to request identification information from the destination device (see figure 5, reference number 506 of Kohn et al.); and
- If the identification information is received from the display device, determining from the identification information, if the destination device is an encryption capable device (see figure 5, reference number 506 of Kohn et al.).

Regarding claim 11, Thue as modified by Maeshima et al. in view of Kohn et al. teaches:

If no identification information is received in a pre-selected period of time after requesting identification information, restricting the output of the source device over the first, second, and third lines to unencrypted video signals which are not subject to restrictions prohibiting their transmission in unencrypted form over analog transmission lines, the unencrypted video signals being fourth, fifth, and sixth video signals.

Although this is not explicitly taught by the combination of Thue/Maeshima et al. in view of Kohn et al., it is understood in an encryption/decryption device that if the decryption device (destination device or display adapter) cannot decrypt the data properly, for whatever reason, the data is sent in its unencrypted form.

Regarding claim 12, Thue as modified by Maeshima et al. in view of Kohn et al. teaches:

- The identification information received from the destination device includes a digital certificate confirming identity of the destination device if the destination device is an encryption capable device (see figure 5, reference number 506 of Kohn et al.); and
- Wherein determining if the destination device is an encryption capable device includes the act of checking the received identification information to determine if said received identification information includes said digital certificate (see figure 5, reference number 506 of Kohn et al.).

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Thue as modified by Maeshima et al. and Kohn et al., further in view of Video Scrambling & Descrambling for Satellite & Cable TV (herein after referred to as VSDSCTV).

Thue as modified by Maeshima et al. and Kohn et al. teaches all the limitations of claims 1-5, as noted above, but the combination system does not disclose transmitting session key information during a video blanking period.

VSDSCTV teaches session key information is transmitted to the destination device during a video blanking period (chapter 1, page 2, under Standard NTSC Format).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to transmit the session key information during a video blanking period, as taught by VSDSCTV, to the method of Thue as modified by Maeshima et al. and Kohn et al. It would have been obvious to transmit the key during that time as taught by VSDSCTV with the method of Thue as modified by Maeshima et al. and Kohn et al. because data transmitted during video blanking is not displayed on the CRT monitor. This also allows the session key, which has to be transmitted anyway, to be done at a time where video synchronization is performed, thus saving time by performing key transmission during an already occurring event.

Claims 13 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thue as modified by Maeshima et al. in view of Kohn et al., and further in view of 5C Digital Transmission Content Protection White Paper, hereinafter referred to as 5CDTCPWP.

Regarding claim 13, Thue as modified by Maeshima et al. in view of Kohn et al. teaches all the subject matter of claims 9, 10 and 11, as noted above. Thue as modified by Maeshima et al. in view of Kohn et al. does not disclose storing session keys used to encrypt video data on the display adapter, and limiting export of video data subject to copy constraints to video data that is in encrypted form.

5CDTCPWP teaches:

- Storing session keys used to encrypt video data on the display adapter (figure 1, the Authentication and Key Exchange Subsystem); and
- Limiting export of video data subject to copy constraints to video data that is in encrypted form (figure 1, the Authentication and Key Exchange Subsystem).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the storage of session keys on the display adapter and the means for limiting export of video data subject to constraints to video data that is in an encrypted form, as taught by 5CDTCPWP, to the device of Thue as modified by Maeshima et al./Kohn et al. It would have been obvious to combine the storage of session keys on the display adapter and the means for limiting export from the device of video data to video data that is in an encrypted form as taught by 5CDTCPWP to the device of Thue as modified by Maeshima et al./Kohn et al. because storage of the session keys on the display adapter would, first, put the session keys on the source device, and second, having the session keys placed on a hardware device would be somewhat tamper resistant (see page 4, last paragraph of 5CDTCPWP); and the

means for limiting export of video data subject to constraints to video data that is in an encrypted form would properly authenticate certain data as copy-once, never copy, etc. (see page 6, table 1 of 5CDTCPWP).

Regarding claim 14, Thue as modified by Maeshima et al./Kohn et al. teaches all of the subject matter of claim 13, as discussed above. However, Thue as modified by Maeshima et al./Kohn et al. does not disclose interfacing with electronic devices through a 1394 interface.

5CDTCPWP teaches interfacing with electronic devices through a 1394 interface (figure 1).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to interface with electronic devices through a 1394 interface, as taught by 5CDTCPWP to the method of Thue as modified by Maeshima et al./Kohn et al. It would have been obvious to interface with electronic devices through a 1394 interface as taught by 5CDTCPWP to the method of Thue as modified by Maeshima et al./Kohn et al. because the 1394 interface provides a means for fast communication between digital electronic devices.

Claims 15-19, 21-29, 31-35, 53, and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kohn et al. in view of Maeshima et al.

Regarding claim 15, Kohn et al. teaches a method of generating encrypted analog first, second and third signals (R', G', B', respectively) from first, second, and third analog input signals (R, G, B, respectively) the method comprising (figure 9):

- Using an encryption circuit (figure 8, reference number 121).

Kohn et al. does not teach:

- Pseudo-randomly generating at least one of a plurality of matrix coefficients, a1, a2, a3, b1, b2, b3, c1, c2, c3; and
- Using the encryption circuit to perform a matrix multiplication operation to generate the encrypted analog first, second, and third signals, according to the following equations:
  - R' = a1R + b1G + c1B
  - G' = a2R + b2G + c2B
  - B' = a3R + b3G + c3B.

Maeshima et al. teaches:

- Pseudo-randomly generating at least one of a plurality of matrix coefficients, a1, a2, a3, b1, b2, b3, c1, c2, c3 (figure 2, reference numbers ra, rb, and rc); and
- Using the encryption circuit to perform a matrix multiplication operation to generate the encrypted analog first, second, and third signals, according to the following equations:
  - R' = a1R + b1G + c1B

- G' = a2R + b2G + c2B
- B' = a3R + b3G + c3B (column 4, top of page). [R', G', and B' are equal to Rdm, Gdm, and Bdm, respectively. R, G, and B are equal to Rd, Gd, and Bd, respectively. a through i, in the reference, are representative of a1 through c3.]

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the pseudo-randomly generated matrix coefficients and the matrix multiplication operation using the coefficients, as taught by Maeshima et al., to the method of Kohn et al. It would have been obvious to combine the pseudo-randomly generated matrix coefficients and the matrix multiplication operation using the coefficients as taught by Maeshima et al. to the method of Kohn et al. because the pseudo-randomly generated matrix coefficients give a randomness to the encryption and the matrix multiplication operation using the coefficients allows a way to modify the red, green, and blue signals in order to encrypt the video signals (see column 3, lines 21-23 of Maeshima et al.).

Regarding claim 23, Kohn et al. as modified by Maeshima et al. teaches the method further comprising:

- Communicating with a destination device to establish a content encryption key to be used as an input to the pseudo-random number generator (see figure 8, reference number 135 going into number 151 of Kohn et al.).

Regarding claim 24, Kohn et al. as modified by Maeshima et al. teaches the method further comprising:

- Using a different content encryption key when encrypting portions of the first, second and third video signals which correspond to different lines of an image (see figure 6, reference numbers 555 and 560 of Kohn et al.).

Regarding claims 25 and 35, Kohn et al. teaches a communication method comprising the steps of:

- Using a pseudo-random number generator to generate output values (figure 9, reference number 200); and
- Transmitting the first, second and third encrypted analog signals to a destination device (figure 8, reference number 130 or 135).

Kohn et al. does not teach modifying first, second and third signals, by performing a matrix multiplication operation thereon utilizing matrix coefficients which are a function of at least one of the pseudo-random output values, the modified first, second and third signals being encrypted analog signals so as to define first, second and third encrypted analog signals.

Maeshima et al. teaches modifying first, second and third signals, by performing a matrix multiplication operation thereon utilizing matrix coefficients which are a function of at least one of the pseudo-random output values, the modified first, second and third

signals being encrypted analog signals so as to define first, second and third encrypted analog signals (figure 1, reference number 50).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the matrix multiplication for encryption of the three analog signals, as taught by Maeshima et al., to the communication method of Kohn et al. It would have been obvious to combine the matrix multiplication for encryption of the three analog signals as taught by Maeshima et al. to the communication method of Kohn et al. because the matrix multiplication allows a way to modify the red, green, and blue signals in order to encrypt the video signals (see column 3, lines 21-23 of Maeshima et al.).

Regarding claim 35 specifically, Kohn et al. teaches a computer readable medium comprising computer executable instructions for controlling a computer device to perform the steps as taught by Kohn et al. in the rejection of claim 25 (figure 8, reference number 122).

Regarding claims 16-18 and 26, Kohn et al. as modified by Maeshima et al. teaches the matrix coefficients correspond to a 3X3 array of matrix coefficients, each row of coefficients including two coefficients of the same value and one coefficient of a different value (see column 4, top illustration of Maeshima et al.). Although Maeshima et al. does not teach each row consisting of two of the same value and one of a different

value, it is known in the art that the three primary colors, RGB, represented in a matrix, contain one 1 and two 0's. More specifically, red = [1,0,0], green = [0,1,0], and blue = [0,0,1].

Regarding claims 19 and 27, Kohn et al. as modified by Maeshima et al. teaches the two coefficients of the same value are positive valued coefficients and the one coefficient of a different value is a negative value coefficient. As can be seen from the rejection of claim 26, each matrix color value consists of two positive 0's and one negative 1. It is understood in the art that a binary 0 represents a positive value and a binary 1 represents a negative value.

Regarding claims 21, 22, and 28, Kohn et al. as modified by Maeshima et al. teaches the matrix multiplication operation includes the act of performing a plurality of analog signal multiplication operations (see figure 2, reference numbers 501, 502, & 503 and column 4, top of page of Maeshima et al.). The matrix shown displays the matrix multiplication values. As can be seen, the signals are red, green, and blue.

Regarding claim 29, Kohn et al. as modified by Maeshima et al. teaches the matrix multiplication operation further includes the act of performing a plurality of analog signal addition operations (see figure 2, reference numbers 504 and 505 of Maeshima et al.).

Regarding claim 31, Kohn et al. as modified by Maeshima et al. teaches:

- Establishing an encryption key with the destination device (see figure 6, reference number 529 of Kohn et al.); and
- Using the encryption key as an input to the pseudo-random number generator, said one pseudo-random output value being generated as a function of the encryption key (see figure 6, reference number 530 of Kohn et al.).

Regarding claim 32, Kohn et al. as modified by Maeshima et al. teaches operating the destination device to decrypt the first, second and third encrypted analog signals utilizing the encryption key (see figure 7 of Kohn et al.).

Regarding claim 33, Kohn et al. as modified by Maeshima et al. teaches wherein operating the destination device to decrypt the first, second and third encrypted analog signals comprises the act of performing a matrix multiplication operation on the first, second and third encrypted analog signals utilizing matrix coefficients generated from said at least one pseudo-random output value (see rejection of claim 25). It is well known in the art of encryption that the process performed on the encryption side is very similar to the process performed on the decryption side. With that knowledge, one skilled in the art would appreciate that, because matrix multiplication was performed for encryption, that matrix multiplication is performed for decryption.

Regarding claim 34, Kohn et al. as modified by Maeshima et al. teaches:

- The destination device is a display device (see figure 8, reference number 160 of Kohn et al.),
- The first, second and third signals are red, green and blue video signals, respectively (see figure 9 of Kohn et al.), and
- The source device is a display adapter (see figure 8, reference number 152 of Kohn et al.).

Regarding claim 53, Kohn et al. teaches a method of generating an encrypted analog signal from at least two of a first analog input signal, a second analog input signal, and a third analog input signal, the method comprising:

- Pseudo-randomly generating an encryption value (figure 9, ref. number 200).

Kohn et al. does not teach:

- Multiplying a first one of said first, second, and third analog input signals with said encryption value to produce a multiplied signal; and
- Combining said multiplied signal with at least a second signal generated from a second one of said first, second, and third analog input signals to produce said encrypted analog signal.

Maeshima et al. teaches:

- Multiplying a first one of said first, second, and third analog input signals with said encryption value to produce a multiplied signal (figure 2, reference number 501, 502, or 503); and
- Combining said multiplied signal with at least a second signal generated from a second one of said first, second, and third analog input signals to produce said encrypted analog signal (figure 2, reference numbers 504 or 505).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to multiply a first signal with the encryption value and to combine that signal with at least a second signal to produce an encrypted analog signal, as taught by Maeshima et al., to the method of Kohn et al. It would have been obvious to combine multiplying a first signal with the encryption value and to combine that signal with at least a second signal to produce an encrypted analog signal as taught by Maeshima et al. to the method of Kohn et al. because multiplying and combining (adding) signals together in an encryption system for analog video would provide a very secure (difficult to break because of the multiplying and adding being performed) encrypted data for transmission.

Regarding claim 54, Kohn et al. as modified by Maeshima et al. teaches wherein said multiplying and said combining are performed as part of a matrix multiplication operation (see figure 2 of Maeshima et al.).

Claims 38 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kohn et al. in view of 5CDTCPWP.

Regarding claim 38, Kohn et al. teaches the device further comprising:

- Video processor circuitry for processing received video signals (figure 8, reference numbers 152 and 160);

Kohn et al. does not teach:

- An additional input/output interface for coupling the video processor to a system bus and a IEEE 1394 compliant bus; and
- A content cipher subsystem for encrypting and decrypting information communicated over the IEEE 1394 compliant bus.

5CDTCPWP teaches:

- An additional input/output interface for coupling the video processor to a system bus and a IEEE 1394 compliant bus (see figure 1 of 5CDTCPWP); and
- A content cipher subsystem for encrypting and decrypting information communicated over the IEEE 1394 compliant bus (see figure 1 of 5CDTCPWP).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the IEEE 1394 compliant capabilities, as taught by 5CDTCPWP, to the device of Kohn et al. It would have been obvious to combine the additional IO interfaces and a content cipher subsystem for handling IEEE 1394 data as

taught by 5CDTCPWP to the device of Kohn et al. because IEEE 1394 compliance, such as those shown by 5CDTCPWP are typically required in a device to be compliant with digital transmission content protection (see page 4, first paragraph of 5CDTCPWP).

Regarding claim 39, Kohn et al. in view of 5CDTCPWP teaches the device further comprising:

- A physically secure non-volatile memory device for storing encryption keys (see figure 1 of 5CDTCPW, the Authentication and Key Exchange Subsystem); and
- Means for limiting export from the device of video data, subject to copy restrictions, received in encrypted form over the IEEE 1394 bus to video data that is in an encrypted form (see figure 1 of 5CDTCPW, the Authentication and Key Exchange Subsystem).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the physically secure key storage device and the means for limiting export from the device of video data to video data that is in an encrypted form, as taught by 5CDTCPWP, to the device of Kohn et al. It would have been obvious to combine the physically secure key storage device and the means for limiting export from the device of video data to video data that is in an encrypted form as taught by 5CDTCPWP to the device of Kohn et al. because a physically secure non-volatile memory device would prevent intruders from tampering with the keys (see page 4, last sentence of last paragraph of 5CDTCPWP) and the means for limiting export

from the device of video data to video data that is in an encrypted form would properly authenticate certain data as copy-once, never copy, etc. (see page 6, table 1 of 5CDTCPWP).

Claim 40 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kohn et al. as modified by 5CDTCPWP, in view of Maeshima et al.

Kohn et al. as modified by 5CDTCPWP teaches all of the subject matter of claim 39, as discussed above. However, Kohn et al. as modified by 5CDTCPWP does not disclose the video signal encryption circuit comprising a matrix multiplier for performing matrix multiplication operations on the red, green, and blue video signals.

Maeshima et al. teaches the video signal encryption circuit comprises a matrix multiplier for performing a matrix multiplication operation on the red, green and blue video signals (see figure 2, reference numbers 501, 502, and 503 of Maeshima et al.).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the video signal encryption circuit comprising a matrix multiplier for performing matrix multiplication operations on the red, green, and blue video signals, as taught by Maeshima et al. to the method of Kohn et al. as modified by 5CDTCPWP. It would have been obvious to combine the video signal encryption circuit comprising a matrix multiplier for performing matrix multiplication operations on the red, green, and blue video signals as taught by Maeshima et al. to the method of Kohn et al. as modified by 5CDTCPWP because the video signal encryption circuit comprising a

matrix multiplier for performing matrix multiplication operations on the red, green, and blue video signals allows a way to modify the red, green, and blue signals in order to encrypt the video signals (see column 3, lines 21-23 of Maeshima et al.).

Allowable Subject Matter

10. Claims 20, 30, and 55 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claims 41-52 are allowed. The prior art of record, or that encountered while searching, fails to anticipate or suggest, alone or in combination, the features of:

- Decrypting the encrypted analog signals by:
    - Generating a third decrypted analog signal from a third pair of encrypted analog signals by:
        - Summing the two encrypted analog signals in the third pair of analog signals to produce a third sum; and
        - Dividing the third sum by a third value to produce a third decrypted analog signal.
- Periodically changing the value used for the first, second and third values as a function of the output of a pseudo random number generator.
- Comparing values in first and second rows of values to identify a first column of values in which the first and second rows of values include the same value.

- Controlling which one of a plurality of output lines the first decrypted analog signal is transmitted on as a function of the identified column of values.
- Comparing values in first and second rows of values to identify a first column in which the first and second rows of values include the same value.
- Comparing values in second and third rows of values to identify a second column in which the second and third rows of values include the same value, the second column being different than said first column.
- Controlling which one of a plurality of output lines the first decrypted analog signal is transmitted on as a function of the identified first column and which one of the plurality of output lines the second decrypted analog signal is transmitted on as a function of the identified second column, the first and second decrypted analog signals being transmitted on different output lines.
- Comparing values in a third row of values and said first row of values to identify a third column in which the third and first rows of values include the same value.
- Controlling which one of a plurality of output lines the third decrypted analog signal is transmitted on as a function of the identified third column, the third decrypted analog signal being transmitted on a different output line from said first and second decrypted analog signals.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Both Copy Protection for High-Definition Baseband Video and Copy Protection System presentation materials present the problem at hand and offer suggestions as to how to solve the problem of protecting the analog video content in a digital video system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 703-305-4662. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Safet Metjahic can be reached on 703-308-1436. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Brandon Hoffman

BH
10/17/03

SAFET METJAHIC
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100